REMARKS

This application contains claims 1-108. Claims 2, 3, 27, 36, 37, 61, 70, 71 and 95 have been canceled without prejudice. Claims 1, 16, 17, 25, 35, 50, 51, 59, 69, 84, 85 and 93 are hereby amended, and new claims 103-108 are added. No new matter has been introduced. Reconsideration is respectfully requested.

Claims 1, 3, 16, 17, 35, 37, 50, 51, 69, 71, 84 and 85 were rejected under 35 U.S.C. 112, second paragraph, for use of language that the Examiner considered to be unclear. Claims 3, 37 and 71 have been canceled, as noted above. Applicant has amended claims 16, 17, 50, 51, 84 and 85 in order to overcome the rejection. Applicant respectfully traverses the rejection of claims 1, 35 and 69.

Claims 1, 35 and 69 were rejected because it was "unclear to the Examiner what are the respective baseline characteristics of the communication traffic." It is not clear to Applicant which term the Examiner felt to be unclear: "baseline" or "characteristics"? "Baseline" is a well-known term of art, which would have been clearly understandable to a person of ordinary skill in the art at the time this application was filed. *Webster's Third New International Dictionary* defines "baseline" as meaning "a known quantity used as a control for further experimentation," and this is plainly the sense in which the term is used in these claims. "Baseline" is also used in this sense in the specification of the present patent application (paragraph 0070 in the published version of the application, US 2005/0021740), as well as by Lyle (U.S. Patent 6,886,102, col. 8, lines 18-20, cited by the Examiner).

"Characteristics" of communication traffic that may be monitored would likewise have had a clear meaning to persons of ordinary skill in the art. Exemplary

characteristics are listed in paragraph 0008 of the specification and are recited in the dependent claims (such as claims 4-9). Lyle uses the term "characteristics" in a similar sense (col. 14, lines 13-19). Moreover, claims 1, 35 and 69 further clarify the scope of the term "characteristics" by requiring explicitly that these characteristics be such that a deviation of the characteristics "is indicative that at least a portion of the communication traffic is of potentially malicious origin."

Thus, Applicant believes that the rejection of claims 1, 35 and 69 under 35 U.S.C. 112 should be withdrawn.

Claims 1-11, 21, 22, 25-45, 55, 56, 59-79, 89, 90 and 93-102 were rejected under 35 U.S.C. 102(e) over Lyle (U.S. Patent 6,886,102). Applicant has amended independent claims 1, 25, 35, 59, 69 and 93 in order to clarify the distinction of the present invention over the cited art. Applicant respectfully traverses the rejection of claims 29-34, 63-68 and 97-102.

Lyle describes a system and method for protecting a computer network against denial of service attacks. One element of this system is a sniffer module, which is "used to monitor network traffic at the ports of devices throughout the network…, to identify messages related to a known or suspected attack or to identify messages that satisfy certain pre-configured criteria believed to indicate the likelihood or possibility that an attack is taking place" (col. 7, lines 39-45). Functions performed by the sniffer module may include searching for predefined strings, as well as searching for "other information, clues, or signatures previously associated with attacks," such as messages sent from suspicious source addresses or messages attempting to access a target system "via a service known to be vulnerable" (col. 10, lines 30-43). Sniffers may also monitor switch

and router ports "to detect if a particular port is receiving an unusually high number of data packets of any type, a high number of data packets of a particular type, and/or a high number of packets with a certain target destination or recipient address" (col. 10, lines 44-49). A statistics database may be used to determine whether the rate of certain types of messages exceeds a normal level (col. 10, lines 52-55).

Claim 1 has been amended to incorporate the limitations of claims 2 and 3, now canceled, with clarification to overcome the rejection of claim 3 under 35 U.S.C. 112. The amended claim recites a method for processing communication traffic that is directed to a group of addresses on a network, in which the traffic that is directed to a subset of the group is monitored. When the characteristics of the traffic directed to at least one of the addresses in the subset deviates from a baseline - indicating that at least a portion of the traffic is of potentially malicious origin - the traffic that is directed to all of the addresses in the group is filtered so as to remove at least some of the malicious traffic. The amended claim language specifies that the subset of the group of the addresses is identified such that the addresses in the subset are expected to receive smaller amounts of the communication traffic than other addresses in the group. Details and rationale for identifying the subset of addresses to monitor in this manner are presented in paragraphs 0008, 0061 and 0062 in the specification.

Lyle neither teaches nor suggests any particular criterion for selection of ports or addresses to be monitored by his sniffer. Intuitively, one would be inclined to connect the sniffer to ports with relatively high volumes of communication traffic, in order to enlarge the volume of data packets that the sniffer can evaluate and thus more readily detect attacks. Lyle

certainly makes no suggestion that the opposite approach should be taken, as required by amended claim 1. The passage in Lyle that was cited by the Examiner against claim 3 (col. 14, line 56 - col. 15, line 30) relates to determining whether a given event is related to an existing incident (col. 14, lines 54-56). It has nothing to do with identifying addresses to be monitored, and certainly does not suggest identifying addresses that are expected to receive small amounts of traffic as recited in claim 1.

Therefore, claim 1, as amended, is believed to be patentable over the cited art. In view of the patentability of claim 1, dependent claims 4-11, 21 and 22 are also believed to be patentable.

Claims 35, 38-45, 55, 56, 69, 72-79, 89 and 90 recite apparatus and computer software products that operate on principles similar to the methods of claims 1, 4-11, 21 and 22. Independent claims 35 and 69 have been amended in like manner to claim 1. Therefore, claims 35, 38-45, 55, 56, 69, 72-79, 89 and 90 are believed to be patentable for the reasons explained above with respect to claim 1.

Independent claim 25 has been amended to incorporate the limitations of claim 27, now canceled. The amended claim recites a method for processing communication traffic in which traffic originating from a group of addresses is monitored in order to detect a pattern that is indicative of a malicious program running on a computer at one (or more) of the addresses. A route of the traffic is traced back to the address so as to identify a location of the computer. The pattern is detected by determining that the computer has transmitted packets to a large number of different destination addresses. This sort of pattern is characteristic, *inter alia*, of certain worm infections.

Lyle describes methods by which an attack can be tracked back to identify the point of attack (col. 8, line 40 - col. 9, line 6). He neither teaches nor suggests, however, applying the specific sort of detection criterion that is recited in amended claim 25. One of Lyle's criteria for discovering an attack is detecting "a high number of packets with a certain target destination or recipient address" (col. 10, lines 48-49, emphasis added), but he gives no suggestion of the opposite criterion recited in claim 25: packets directed to many different destination addresses.

The passage in Lyle that was cited by the Examiner against claim 27 (col. 13, lines 9-21) relates to the manner in which an "event manager" module "meters the amount of data and the rate at which data is provided to the analysis framework." The purpose of this metering is to prevent multiple messages to one destination from masking another message to a different destination (lines 16-18). It is an internal function of Lyle's system, which has nothing to do with determining that a suspect computer has transmitted packets to a large number of different destination addresses, let alone using the large number of different destination addresses as a pattern indicative of a malicious program running on the computer, as recited in amended claim 25.

Thus, claim 25 is believed to be patentable over the cited art. In view of the patentability of claim 25, dependent claims 26 and 28 are also believed to be patentable.

Claims 59, 60, 62, 93, 94 and 96 recite apparatus and computer software products that operate on principles similar to the methods of claims 25, 26 and 28. Independent claims 59 and 93 have been amended in like manner to claim 25. Therefore, claims 59, 60, 62, 93, 94 and 96 are believed to be patentable for the reasons explained above with respect to claim 25.

Independent claim 29 recites a method in which communication traffic is monitored so as to detect packets indicative of a network communication failure that is characteristic of a worm infection. Upon detecting an increase in the rate of arrival of these packets, the communication traffic is filtered so as to remove at least a portion of the communication traffic that is generated by the worm infection. One type of packets that are indicative of communication failures of this sort is "ICMP unreachable" packets, as recited in dependent claim 30 and explained in the specification (paragraph 0065).

Lyle makes no mention or suggestion of communication failures or how they should be handled, and does not even hint that packets indicative of such failures could be used in filtering worm-generated traffic as required by claim 29. The passage in Lyle that the Examiner cited against claim 29 (col. 10, line 53 - col. 11, line 1) relates only to "certain types of messages" (lines 55-56), without specifying the types of messages that are involved. MPEP 2131 states:

> TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California* ,814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)... "The identical invention must be shown in as complete detail as is contained in the... claim." *Richardson v. Suzuki Motor Co*., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

In the absence of any mention in Lyle of "packets that are indicative of a communication failure," it is clear that Lyle fails to meet the burden of MPEP 2131. With

regard to claim 30, Lyle also contains no teaching or suggestion at all of ICMP.

Thus, independent claim 29 is believed to be patentable over the cited art. In view of the patentability of claim 29, dependent claims 30 and 31 are also believed to be patentable.

Claims 63-65 and 97-99 recite apparatus and computer software products that operate on principles similar to the methods of claims 29-31. Therefore, claims 63-65 and 97-99 are believed to be patentable for the reasons explained above with respect to claim 29.

Independent claim 32 recites a method in which communication traffic on a network is monitored so as to detect ill-formed packets. The ill-formed packets are used in determining that at least a portion of the traffic has been generated by a worm infection. The communication traffic is then filtered in order to remove at least the portion of the worm-generated traffic. Examples of ill-formed packets are described in the specification (paragraphs 0066-0068) and are recited in dependent claims 33 and 34.

Lyle fails to relate in any way to whether packets are well formed or ill formed, and certainly does not suggest that detection of ill-formed packets might be used in determining that a worm infection has occurred. The passage cited by the Examiner against claim 32 (col. 7, lines 9-19) says only that "the sniffers search for data indicating an actual or suspected attack... as described more fully below." Lyle describes a number of ways in which the sniffers may search for such attack-related data (see, for example, col. 10, lines 30-59). None of these ways has anything to do will ill-formation of packets.

Thus, Applicant respectfully submits that Lyle fails to meet the burden of MPEP 2131, as cited above, with respect to claim 32. Claim 32 is therefore believed to

be patentable over the cited art, as are claims 33 and 34, which depend from claim 32.

Claims 66-68 and 100-102 recite apparatus and computer software products that operate on principles similar to the methods of claims 32-34. Therefore, claims 66-68 and 100-102 are believed to be patentable for the reasons explained above with respect to claim 32.

Dependent claims 12-20, 23, 24, 46-54, 57, 58, 80-88, 91 and 92 were rejected under 35 U.S.C. 103(a) over Lyle in view of Porras (U.S. Patent 6,321,338) or Trcka (U.S. Patent Application Publication 2001/0039579). In view of the patentability of independent claims 1, 35 and 69, from which these claims depend, dependent claims 12-20, 23, 24, 46-54, 57, 58, 80-88, 91 and 92 are also believed to be patentable.

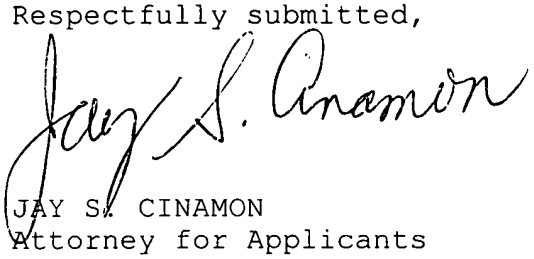
Notwithstanding the patentability of the independent claims in this application, as explained above, the dependent claims are also believed to recited independently-patentable subject matter. In the interest of brevity, however, Applicant will refrain from arguing the patentability of the dependent claims at present.

New dependent claims 103-108 have been added to more completely recite the features of the present invention. These claims depend from independent claims 1, 35 and 69, respectively, and recite criteria according to which addresses may be selected for inclusion in the monitored subset. These claims are literally supported in paragraphs 0061 and 0062 of the specification. The prior art neither teaches nor suggests these sorts of selection criteria.

Applicant believes the amendments and remarks stated above to be fully responsive to all of the grounds of rejection raised by the Examiner. In view of these amendments and remarks, all the claims in the present patent application are believed to be in condition for allowance. Prompt notice to this effect is requested.

Please charge any fees which may be due, and which have not been submitted herein, to our Deposit Account No. 01-0035.

Respectfully submitted,



JAY S. CINAMON
Attorney for Applicants
Reg. No. 24,156

ABELMAN, FRAYNE & SCHWAB
666 Third Avenue, 10th Floor
New York, New York 10017
(212) 949-9022
(212) 949-9190

Colb\7 19 06 bar.amt